(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－130378

(43)公開日　平成９年(1997) ５月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ１		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ａ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ
		６６０	7259－5Ｊ			６６０Ｅ
Ｈ０４Ｌ	9/20			Ｈ０４Ｎ	7/16	
Ｈ０４Ｎ	7/16			Ｈ０４Ｌ	9/00	６５３

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平8－242040

(22)出願日　平成８年(1996) ９月12日

(31)優先権主張番号　９５１０８４２

(32)優先日　1995年９月15日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　391000771
トムソン　マルチメデイア　ソシエテ　アノニム
THOMSON MULTIMEDIA S. A.
フランス国　クールベボワ　ラ・デフアンス　５　プラス・デ・ボージュ　９

(72)発明者　ジャン－ベルナール　フィッシャー
フランス国　35700　レンヌ　リュ・ド・ヴァンセンヌ　９ア

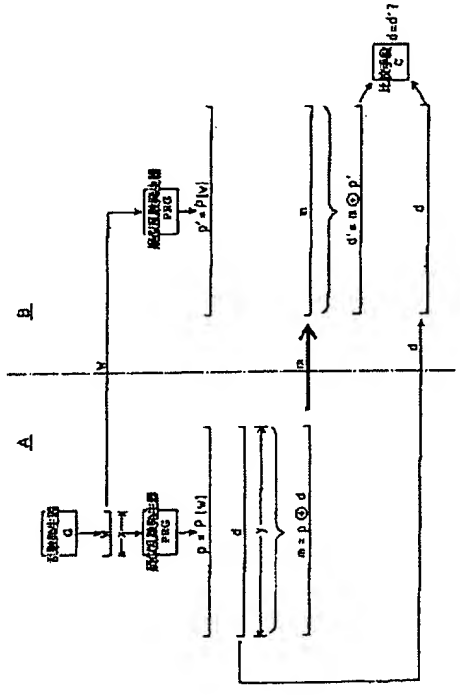
(74)代理人　弁理士　伊東　忠彦　（外１名）

(54)【発明の名称】　安全なデータ交換プロトコルのデータを保証する方法

(57)【要約】

【課題】　本発明は記憶及び計算資源の使用量が削減されたデータ保証方法を提供する。

【解決手段】　本発明の方法は、送信者が疑似ランダム語を生成すべく疑似乱数発生器に供給されるシードを生成し、チェック語を生成すべく１対１の不可逆的な疑似ランダム語を被担保データ項目と合成し、チェック語を受信者に伝送する保証段階と、送信者が平文被担保データ項目とシードを受信者に伝送し、受信者が別の疑似ランダム語を生成すべく送信者側の疑似乱数発生器と類似した疑似乱数発生器にシードを供給し、チェックデータ項目を生成すべく送信者側と同様に別の疑似ランダム語をチェック語と合成し、チェックデータ項目と平文被担保データ項目の整合性をチェックする開始段階とからなる。



【特許請求の範囲】
【請求項１】　保証されたデータ項目を１対１ではあるが不可逆的な形で表わし、上記保証されたデータ項目のイメージであるデータ項目を、受信者に伝送するような態様で、上記保証されたデータ項目の所有者である送信者が上記受信者と情報を交換する保証段階と、
平文の保証されたデータ項目を上記受信者に伝送するような態様、或いは、上記平文の保証されたデータ項目が得られる態様で、上記送信者が上記受信者と情報を交換し、上記受信者が、上記保証段階の上記データ項目との上記保証されたデータ項目の整合性を照合することができる開始段階とからなる安全なデータ交換プロトコルのデータを保証する方法であって、
上記保証段階において、上記送信者が、
疑似ランダム語を生成するような態様で、疑似乱数発生器に供給されるシードを生成し、
チェック語を生成するような態様で、１対１の不可逆的な形で上記疑似ランダム語を上記保証されたデータ項目と合成し、
上記チェック語を上記受信者に伝送し、
上記開始段階において、上記送信者が、
上記平文の保証されたデータ項目と共に上記シードを上記受信者に伝送し、
上記シード及び上記保証されたデータ項目を受信した際に、上記受信者が、
別の疑似ランダム語を生成するような態様で、上記送信者の上記疑似乱数発生器と類似した疑似乱数発生器に上記シードを供給し、
チェックデータ項目を生成するような態様で、上記送信者と同じ１対１の不可逆的な形で上記別の疑似ランダム語を上記チェック語と合成し、
上記送信者から受信された上記平文の保証されたデータ項目と上記チェックデータ項目の整合性をチェックすることを特徴とするデータを保証する方法。
【請求項２】　上記送信者及び上記受信者の上記夫々の疑似乱数発生器によって生成された上記疑似ランダム語及び上記別の疑似ランダム語は、上記保証されたデータ項目と同じ長さ（ｙ）の語であり、
上記１対１の不可逆的な合成演算は排他的論理和である請求項１記載のデータを保証する方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は安全なデータ交換プロトコルのデータを保証する処理に関する。本発明は、例えば、コンピュータネットワーク、又は、条件付きのアクセステレビジョン（有料テレビジョン、符号化されたテレビジョン等）の照合システムにおいて、特に、物理的及び論理的なアクセス制御システムへの応用の際に有利である。勿論、上記の応用は、それに限定されることはなく、本発明が使用される技術分野の例として挙げられたものに過ぎない。
【０００２】
【従来の技術】データ項目を保証又は担保に入れる原理は、第１の当事者が、所定のデータ項目を明文で通信することなく、第２の当事者に通信することである。次のステップの間に、第１の当事者は、平文のデータ項目を第２の当事者に明かし、第２の当事者は、そのとき、上記平文のデータ項目が実際に予め安全に担保に入れられたものであるかどうかを照合する可能性がある。
【０００３】ここで、用語“当事者”は、特定のプロトコル、或いは、より一般的には、所定の取引の枠組み内で完全に自動的な態様でデータ交換を行う電子又はコンピュータシステムと同様に、精神的又は物理的な人と関係することに注意する必要がある。同様に、取引の主題を形成するデータ項目は、“保証されたデータ項目”又は“被担保データ項目”と呼ばれ、上記被担保データ項目を初期に保有する当事者（上記“第１の当事者”）は“送信者”又は“債務者”と呼ばれ、被担保データ項目が向けられた当事者（上記“第２の当事者”）は“受信者”又は“債権者”と呼ばれる。
【０００４】上記担保プロトコルには以下の幾つかの制約が含まれる。第１に、適当な時間、例えば、共に行われた作業の終結、又は、両当事者間の安全なデータ交換の終了まで、被担保データ項目を債権者（及び、第三者）に対し秘密にしておく必要がある。債務者が、例えば、最初に担保に入れられたデータ項目以外のデータ項目を債権者に明かすことにより、不正、又は、詐欺を行えないことが不可欠である。
【０００５】かかる担保処理は既に提案されている。それらは、一般的に、暗号文ブロック連鎖方式（ＣＢＣモード）のデータ暗号化規格（ＤＥＳ）のような暗号作成ハッシュ関数を用いる。上記関数の説明は、その実施例と共に、ビー　プレネール(B. Preneel)等による“暗号論的に安全なハッシュ関数：概要”、アール　シーメールクル(R.C. Merkle) による“１方向性ハッシュ関数とデータ暗号化規格”、ＬＮＣＳ、Springe Verlag刊行、1990年、４２８－４４６ページ、又は、ジージェー　シモンズ(G.J. Simmons)著の現代暗号理論、ＩＥＥＥプレス刊行、第６章：ディジタル署名に記載されている。
【０００６】
【発明が解決しようとする課題】上記関数の一つの欠点は、それらがかなり多量の記憶容量と、かなり多量の計算能力とを必要とすることから生じ、その欠点は、スマートカードの超小型コントローラ、又は、超小型回路のような制限された寸法の構造と共に上記処理を実現することが望ましいときには許容されない。
【０００７】上記問題点を解決するため、本発明の提案するデータを保証する方法は、かなり少量の記憶資源及び計算資源しか使用しないので、上記スマートカードの超小型回路又は超小型コントローラによって実現可能で

ある利点がある。

【０００８】

【課題を解決するための手段】本発明の方法は上記の周知のタイプのデータを保証する方法の中の方法であって、即ち、被担保データ項目（又は保証されたデータ項目）を１対１ではあるが不可逆的な形で表わし、上記被担保データ項目のイメージであるデータ項目を、債権者（又は受信者）に伝送するような態様で、上記被担保データ項目の所有者である債務者（又は送信者）が上記債権者と情報を交換する担保（又は保証）段階と、平文の被担保データ項目を上記債権者に伝送するような態様、或いは、上記平文の被担保データ項目が得られる態様で、上記債務者が上記債権者と情報を交換し、上記債権者が、上記被担保データ項目の上記担保段階の上記データ項目との整合性を照合することができる開始段階とからなる。

【０００９】本発明によれば、上記データを保証、又は、担保に入れる方法は、上記担保段階において、上記債務者が、疑似ランダム語を生成するような態様で、疑似乱数発生器に供給されるシードを生成し、チェック語を生成するような態様で、１対１の不可逆的な形で上記疑似ランダム語を上記被担保データ項目と合成し、上記チェック語を上記債権者に伝送し、上記開始段階において、上記債務者が、上記平文の被担保データ項目と共に上記シードを上記債権者に伝送し、上記シード及び上記被担保データ項目を受信した際に、上記債権者が、別の疑似ランダム語を生成するような態様で、上記債務者の上記疑似乱数発生器と類似した疑似乱数発生器に上記シードを供給し、チェックデータ項目を生成するような態様で、上記債務者の場合と同じ１対１の不可逆的な形で上記別の疑似ランダム語を上記チェック語と合成し、上記チェックデータ項目の、上記債務者から受信された上記平文の被担保データ項目との整合性をチェックすることを特徴とする。

【００１０】有利な実施例において、上記債務者及び上記債権者の上記夫々の疑似乱数発生器によって生成された上記疑似ランダム語及び上記別の疑似ランダム語は、上記被担保データ項目と同じ長さの語であり、上記１対１の不可逆的な合成演算は排他的論理和である。

【００１１】

【発明の実施の形態】本発明の他の特徴及び利点は、以下の本発明の実施例の詳細な説明を読むことにより明らかになる。第１の当事者Ａ（債務者）は、データ項目ｄを第２の当事者（債権者）に引き渡す義務があり、このデータは、例えば、共同作業が終結、又は、両当事者間の取引が終了するまで一時的に秘密のままにしておく必要がある。

【００１２】上記プロトコルは、本質的に以下の二つの段階、債権者Ｂが、この段階の最後に、データ項目ｄを１対１ではあるが、データ項目ｄをそれ自体から復元し得ないような態様で情報項目（以下、ｍと呼ぶ）を保有するように（確率論的に言うと、ｎが安全パラメータの値を表わす場合に、債権者Ｂが１／ｎを上回る確率でｍからｄを推論可能であってはならない）、債権者Ｂとの担保に入れたいデータ項目ｄを所有する債務者Ａが、債権者Ｂとメッセージを交換する担保段階と、債務者Ａが債権者Ｂに対しデータ項目ｄを明文で明らかにし、債権者Ｂは、この段階中に伝送されたデータ項目が前の段階で安全に担保に入れられたデータ項目と実際に同一であることを確かめることが可能でなければならない（確率論的に言うと、債務者Ａが担保に入れられていない値を明かすことにより詐欺を企てた場合に、少なくとも１－１／ｎの確率で発見可能である）開始段階とを処理する。

【００１３】本質的に、本発明の処理は、疑似乱数発生器、即ち、“シード”と呼ばれるあらゆる入力語に対し、出力としてそれよりも長い語を生成する関数の使用に基づいている。出力語は、決定論的な方法で生成されるが、疑似乱数、即ち、語の初期のビットが分かっていても、シードが分からない限り、次のビットを発見することが実際的に不可能であり、逆に言えば、出力語に基づいてシードを発見することが少なくとも同様に困難である。

【００１４】換言すれば、疑似乱数発生器は、想定された応用、及び、特に、通例の取引時間が与えられた場合に許容されない計算能力及び／又は時間を要求しない限り、逆転させることが困難でなければならない。エスウォルフラム(S. Wolfram)の“セル状オートマトンによる暗号化”、暗号理論の進展(Advences in Cryptology)、１９８５年暗号化講演会(Proc. Crypto '85)、コンピュータサイエンスの講義録、２１８（１９８６年）、ページ４２９－４３２に記載されているような“セル状オートマトン”を、特に、上記の疑似乱数発生器に使用することが可能である。

【００１５】以下、かかるセル形オートマトンが本発明の枠組みに実現された例を説明するが、この実施例は、例として示されているだけであり、この例に限定されることを示すものではない。図１に示されているように、処理に関係した各当事者Ａ及びＢは、ＰＲＧの名前が付けられた疑似乱数発生器のような同一のアルゴリズムに従って動作する２台の発生器を所有する。

【００１６】債務者Ａは、乱数発生器Ｇを更に有する。各当事者Ａ及びＢは、

【００１７】

【外１】

$$\oplus$$

【００１８】によって表わされた１ビットずつの排他的論理和関数を実行可能な手段が設けられている。最後に、債権者Ｂは、入力として供給された２個の語の間の同一性を判定することができる１ビットずつの比較手段

Cを有する（上記語の一致は、取引中に債務者によるデータ変遺が無かったことを証明する）。

【００１９】以下に説明する処理は、上記の如く“担保”及び“開始”の２段階で進められる。担保は、債務者Ａ側で、発生器Ｇによって生成されたランダムな語ｗを得ることにより始まる。上記語ｗは、シードとして疑似乱数発生器ＰＲＧに供給され、疑似乱数発生器ＰＲＧは、そのアルゴリズムに従って、当事者ＡとＢの間で担保に入れるため必要とされるデータ項目ｄと同一の長さの疑似ランダム文字列ｐ＝Ｐ（ｗ）を生成する。

【００２０】債務者Ａは、次に

【００２１】

【数１】

$$m = p \oplus d$$

【００２２】を計算、即ち、（同一の長さの２個のデータ項目）ｐとｄの間の排他的論理和を演算し、要求されるデータ項目ｍを債権者Ｂに伝送する。データ項目ｍはデータ項目ｄの１対１の暗号化された表現であるが、疑似乱数発生器によって生成された文字列ｐを判定することが可能である限り、データ項目ｄは完全に秘密にされ、これが“１回限りの使い捨て鍵(one-time pad)”として周知である排他的論理和の合成の特性であることに

$$d' = m \oplus p'$$

【００２６】を計算し、全ての操作が適切に動作していることを証明する式ｄ’＝ｄ　を照合し、全てが正しく動作しているならば、

【００２７】

【数３】

$$d' = m \oplus p' = (p \oplus d) \oplus p = p \oplus p \oplus d = d$$

【００２８】が得られる。本発明によるプロトコルは、暗号化されたデータ項目ｍだけではなく、平文データ項目ｄとシードｗを伝送する必要があるので、従来のハッシュ関数よりも多数の伝送を必要とすることに注意すべきである。かくして、従来のハッシュ関数の場合に、担保は、６４又は１２８ビットの値に関し操作され、一方、本発明の場合、例えば、データ項目ｄの長さが１０，０００ビットであるならば、少なくとも１０，０００ビットを伝送する必要があるので、本発明は、特に、データ項目が適度の寸法、典型的に１，０００ビット未満の長さである場合（実際上、最も頻度の高い場合）に適している。

【００２９】他方で、本発明の処理は、必要とされるメモリ資源に関し従来のハッシュ関数よりも特に有利であり、ハッシュ関数の場合に、ハッシュされるべきブロックの必要とされるサイズに対応した多数のビット（典型的に、６４又は１２８ビット）を集める必要があり、安全性の観点から屡々非常に望まれるようにデータ項目がより長い場合には、少なくとも新しいブロックと前のハッシュ演算の結果、即ち、１２８乃至２５６ビットをランダムアクセスメモリに保持することが必要である。これに対して、本発明の処理の場合には、望みに応じて小さいブロックでビットを伝送するだけで十分であり、メモリ資源の要求量が対応して低減される。極端な場合には、データを１ビットずつ伝送することが可能であるので、中間記憶装置が必要ではない。

【００３０】プロトコルの安全性に関して、このことが利点であり、実際上、選択された疑似乱数発生器の品質と被担保データ項目の長さだけに依存することが分かる。以下、ｘが疑似乱数発生器のシードのビットの長さを表わし、ｙがデータ項目の長さを表わすことにする。当事者Ｂの観点からは、プロトコルを“解読する”ための唯一の解決法は、シード、或いは、疑似乱数発生器によって出力された語に関する指示を得ることである。しかし、シードはランダムに生成され、かつ、開始までは秘密にされている。従って、当事者Ｂの有する手段は可能性のある全てのシードを系統的に試すことだけであり、当事者Ｂがそのようにできるならば、上記の如く生成されたデータ項目の有効性を照合することにより、実行可能な解を見つけることが可能である。

【００３１】従って、シードは、網羅的な攻撃を排除するためかなり長くされる必要があるので、実現可能な２６４個のシードの下限が固定される。当事者Ａの観点からは、不正の誘発は、魅力的な相手(match) を見つける可能性と関連付けられる。即ち、当事者Ａが被担保データ項目ｄとして欺罔したいと思う虚偽のデータ項目δを有する場合に、当事者Ａが、

注意する必要がある。換言すれば、排他的論理和を適用することによる暗号化は、疑似乱数発生器と同様に安全であり、即ち、外部の監視者（当事者Ｂ又は第三者）は、疑似乱数発生器のシードｗを知ることなくｐを推論する場合に得られる確率よりも高い確率で、ｍからデータ項目ｄを推論し得ない。

【００２３】語ｍが債権者Ｂとの担保に入れられた後、当事者Ａ及びＢは、両者の間で所望の取引を操作し、計画された作業を共に実行すること等により着手されたプロトコルを続ける。上記操作的なフェーズが終了した後、開始段階に進むことが可能である。債務者Ａは、担保段階の最初にこのデータ項目を暗号化する機能を行ったシードｗと共に、担保に入れられたデータ項目ｄを明文で債権者に提示する。

【００２４】当事者Ｂは、自分自身の疑似乱数発生器を用いて、データ項目ｐ’＝Ｐ（ｗ）を計算する（通常、当事者Ａが実際に真のシードを当事者Ｂに伝送した場合には、ｐ＝ｐ’である）。担保に入れられ、かつ、保持されている暗号化されたデータ項目ｍを用いて、当事者Ｂは、次に、排他的論理和関数を用いて、

【００２５】

【数２】

【００３２】
【数４】

$$d \oplus P(\omega) = \delta \oplus P(\omega)$$

【００３３】となるようなωを見つける必要があることを意味し、これは、
【００３４】
【数５】

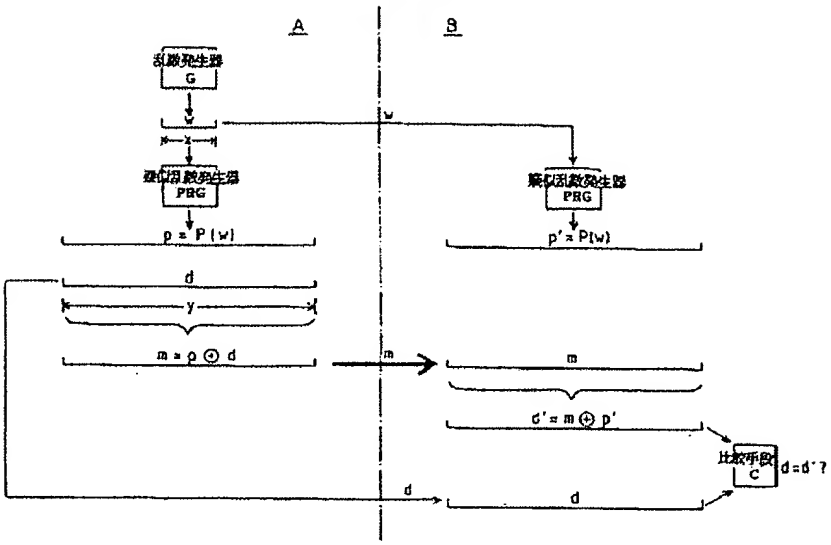
$$P(\omega) = d \oplus P(w) \oplus \delta$$

【００３５】を見つけることと同じであり、従って、疑似乱数発生器からの所定の出力に対応したシードを見つけることである。しかし、この問題は、疑似乱数発生器の固有の特性に起因して困難である。それにも関わらず、出力語の長さが入力語の長さよりも短いならば、所定の出力に対する相手の数は１よりも大きいので、かかる相手が存在するあらゆる機会があることに注意する必要がある。
【００３６】更に、当事者Ａは、取引前に、不正の準備を行い、かつ、魅力的な相手を見つけるために十分な時間を有するが、一方、当事者Ｂは非常に制限された時間（取引のための時間）しかないことに注意することが非常に重要である。従って、当事者Ａの成功の機会を最小限に抑えることが必要である。かくして、例えば、2^{64}通りの実現可能なシードの最小値が保持された場合には、当事者Ａは、マッチを見つける前に、おそらく2^{32}回の試行を処理することが可能であり、この試行は容易に実行されるので、（バースデーパラドックス(birthdays paradox)によって）安全性が十分ではないということに注意する必要がある。
【００３７】しかし、出力語の長さｙがシードの長さｘよりも長い場合には、ある語が発生器によって生成され得る確率は、僅かに$1／2^{y-x}$、即ち、ｙ＝９６かつｘ＝６４の場合に、$1／2^{32}$である。これは、当事者Ａが、疑似乱数発生器によって発生させられた１個の出力語を見つけるために、2^{32}個の異なるδの値を試行しなければならないことを意味し、全部で略$2^{32+32} = 2^{64}$通りの（δ，ω）の対の試行が行われることになり、実際上、達成不可能である。
【００３８】従って、ｘ及びｙの大きさのオーダーとして以下の最小寸法を課すことが可能である。
－シードの長さｘは６０ビットよりも長い。
－被担保データ項目の長さｙは（冗長量の導入を必然的に伴うとしても）１００ビットよりも長い。
【００３９】
【実施例】セル状オートマトンに基づき、かつ、ｉが０＜ｉ≦ｎを表わすとき、ｎ個の位置s_iを含む巡回レジスタにより構成された疑似乱数発生器の場合を例として考える。上記レジスタは、状態関数：
【００４０】
【数６】

$$s_i = s_{i+1} \oplus (s_i \vee s_{i-1})$$

【００４１】の変更を各位置s_iに適用することにより展開される。各巡回毎に、発生器が展開され、位置s_iの値が“出力”される。発生器の初期化は、ある値を各位置に与えることにより行われる。従って、シードの長さはｎである。出力でｋビットが要求されるならば、２．ｎ．ｋ回の基本演算が要求されることに注意する必要がある。
【００４２】上記発生器は、“ＮＰ問題”（ウォルフラムの上記引用文献を参照のこと）に依存しているので安全であり、発生された異なる文字列の数は2^nのオーダーである。寸法の決定に関し、データ項目は２５６ビット長であり、レジスタは６１個の位置からなる。これにより、2^{61}のオーダーの実現可能な出力（パディング(paddings)と呼ばれる）が得られ、２５６ビットからなるある文字列がシードに対応する確率は、2^{-195}、即ち、10^{58}回当たりに１回の機会である。
【００４３】担保の計算は、照合の計算の場合と同様に、３２，０００回の基本操作を要求する。
【図面の簡単な説明】
【図１】本発明の処理を実現するため行われる種々の操作及びデータ交換を概略的に示す図である。
【符号の説明】
Ａ　第１の当事者（債務者）
Ｂ　第２の当事者（債権者）
Ｃ　比較手段
Ｇ　乱数発生器
ＰＲＧ　疑似乱数発生器
ｄ，ｄ’　データ項目
ｍ　情報項目
ｐ，ｐ’　ランダム文字列
ｗ　シード
ｘ　シードの長さ
ｙ　出力語の長さ

【図１】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-130378
(43)Date of publication of application : 16.05.1997

(51)Int.Cl. H04L 9/32
G09C 1/00
G09C 1/00
H04L 9/20
H04N 7/16

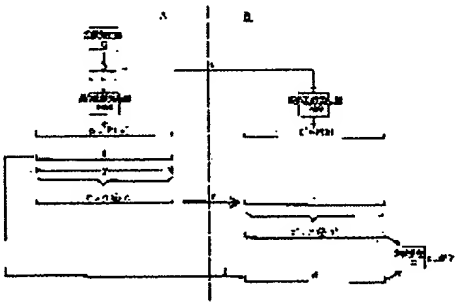
(21)Application number : 08-242040
(22)Date of filing : 12.09.1996

(71)Applicant : THOMSON MULTIMEDIA SA
(72)Inventor : FISCHER JEAN BERNARD

(30)Priority
Priority number : 95 9510842 Priority date : 15.09.1995 Priority country : FR

(54) METHOD FOR ENSURING DATA BY SECURE DATA EXCHANGE PROTOCOL

(57)Abstract:
PROBLEM TO BE SOLVED: To allow even a small amount of a storage resource and calculation resource to be enough for the purpose by collating consistency with data items of security stage for granted data items.
SOLUTION: Concerned parties A, B with the processing have two generators is operation according to the same algorithm such as pseudo random number generators names PKG. A debt party A has also a random number generator G. The concerned particles A, B have a means executing exclusive OR function bit by bit each. Finally the debt party B ha a comparator means C one by one bit to determine the identity between two words received as inputs. Then in the mode of transmission to the debt party (or recipient) A, the debt party (or recipient) A being a possessor of granted data items exchanges information with the debt party B. Moreover, the debt party A exchanges information with the debt party B and the debt party B collates the consistency with the data items in the security stage of the granted data items.



LEGAL STATUS

[Date of request for examination] 09.09.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]